Guest View: SaaS security: Getting it right the first time

Column (https://sdtimes.com/category/column/) **Published: January 3rd, 2017 - Mayur Ramgir (https://sdtimes.com/author/mayur-ramgir/)**

In my previous article, “Why developers are struggling with SaaS (https://sdtimes.com/guest-view-developers-struggling-saas/),” I talked about the three most important building blocks of software-as-a-service (SaaS) architecture: security, performance, and data backup and recovery. Now I want to dive deep into SaaS security. In order to be relevant in today’s dynamic cybersecurity climate, SaaS applications must be hyper-focused on security and the burden of ensuring a secure SaaS platform based on current industry best practices rests solely with you as a developer and architect.

SaaS architects and developers need to be cybersecurity gurus. There are various security measures you can take to ensure your SaaS offering is sustainable and, most importantly, reliable.

Authentication and authorization: The first line of defense

Authentication and authorization, also known as Identity and Access Management (IAM), plays a vital role in securing your application. Architects and developers need to be fully informed on IAM functionality and the web software security model that I will expand upon.

In the first line of defense, you have to make sure that you are only allowing access to authorized individuals. The following are some of the different authentication forms you may use to secure a user’s entry to your SaaS application.

- Simple username and password-based authentication
- 2-factor authentication using an external device
- Biometric authentication like fingerprint scan and retina scan
- PKI-based authentication using public and private keys

Depending on your application domain, you may also need to add more defense layers like restricting access to a specific IP address or a range of IP addresses, MAC addresses, etc.

Authorization: A balance between security and business progress

Authorization plays as important a role as authentication plays. Once the user is authenticated, it is extremely important to make sure he can access whatever he is required to access, but no more and no less.

As an architect you should think about creating a strong authorization model, which not only controls data access, but also other resources like documents. There are various authorization models you can use; however, for SaaS-based architecture, role-based access control is the best for most situations.

An authentication and authorization model should include the following:

- Identity governance services as they relate to compliance, role engineering, and identity-assurance policies
- Access-management services that work in conjunction with identity-management services to grant access based on successful authentication
- Identity-management services based on identity life-cycle-management protocol

For authentication, many organizations like to use single sign-on to connect your application with other applications they may be using internally. So, make sure your SaaS application supports standard single sign-on implementations.

Endpoints: Secure entry point to your application

With application programming interfaces (APIs), and the advent of private and public cloud options within disparate applications, organizations are looking for an integrated solution to consolidate the data they are generating from these standalone applications. They want to make sure the applications they are using are fully interoperable. Therefore, they are expecting you to open your application via APIs, which adds more complexity to your security model. You need to make sure you are not creating any backdoors, which can enable hackers to get into your database and get access to your customers' data. Hence, it is important to take proper measures to secure those endpoints before exposing them to public.

As an architect, you should think about creating innovative strategies and solutions that can secure your application's environment. You must focus on high-level, innovative approaches that consider complex solutions such as encryption in flight, encryption at rest, and IAM across the security spectrum.

Encryption: SSL and beyond

Encryption is another tool you should consider in your arsenal. Since SaaS applications are accessible via the Internet, the data travels from the user's computer to your server. Anyone can listen to the traffic and capture the data. They can also act as a middleman where they will intercept the traffic and relay messages between the user and your server. Both parties in the conversation think that they are talking directly to each other.

However, in reality the conversation is controlled by a third person. This person can collect data, manipulate it and send it to the other party. This type of attack is known as "man-in-the-middle" attack. Hence, you should consider using a secure tunnel to transfer data between the user's computer and your server. This can be done by using an SSL (Secure Sockets Layer) certificate. SSL not only encrypts the data in transit, but it also provides a means to authenticate the receiving party. This way the user's computer will know if it is actually talking to your server or not.

Encryption should be used carefully as it adds overhead. For example, when you encrypt data before storing it in the database, you must decrypt it before your application can process it. This requires additional CPU processing time from your server and may slow down all or part of your application. Hence, you should only consider encrypting the critical part of the data like social security number, credit card number, etc.

SaaS security best practices: Closing points to consider

Consider the following best practices to arrive at the right approach to SaaS security:

- Create strong authentication and authorization policy for your app from the very beginning
- Use consistent app security protocols across the development phase
- Prioritize the architecture and design of your security processes at the outset of your project
- Incorporate security evaluation into the DevOps automation process
- Validate that your apps are sufficiently secure and on par with the specs that you have in place
- Automation of testing is paramount to the successful launch of secure SaaS app
- Consider the ultimate user experience and holistic app performance in your design from the beginning
- Stay on top of your industry's regulatory and security compliance requirements

Use your industry's compliance and regulatory requirements to set the parameters for the level of security and encryption your SaaS app requires. Be sure to fully understand all compliance regulations early on in the process, as it is much more difficult to adjust these policies after they have already been implemented.

In today's ever-evolving world of SaaS security and app development, developers and architects have much on their plate. Keep these tips in mind to stay on the right track and keep your app user-friendly, relevant, and secure.

ARTICLE TAGS

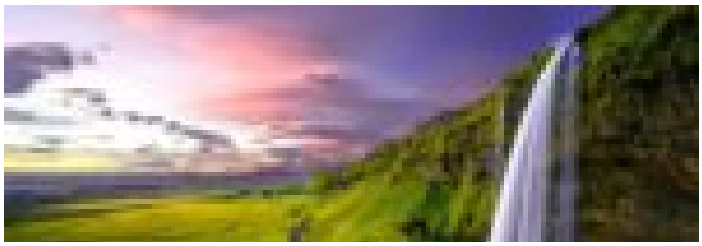
DevOps (https://sdtimes.com/tag/devops/), encryption (https://sdtimes.com/tag/encryption/), Identity Access Management (https://sdtimes.com/tag/identity-access-management/), identity management (https://sdtimes.com/tag/identity-management/), SaaS (https://sdtimes.com/tag/saas/), Secure Sockets Layer (https://sdtimes.com/tag/secure-sockets-layer/), security (https://sdtimes.com/tag/security/), Software-as-a-Service (https://sdtimes.com/tag/software-as-a-service/), SSLs (https://sdtimes.com/tag/ssls/)

About Mayur Ramgir

Mayur Ramgir is president and CEO of Boston-based software development firm Zonopact, a company that specializes in development of high-performance business solutions in the cloud. Zonopact developed the Clintra (http://www.clintra.com) SaaS platform. Reach him at: mramgir@zonopact.com

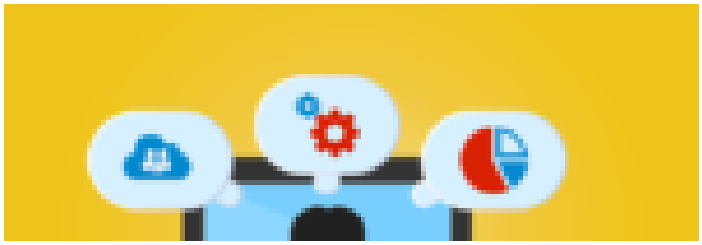
View all posts by Mayur Ramgir (https://sdtimes.com/author/mayur-ramgir/)

RELATED ARTICLES

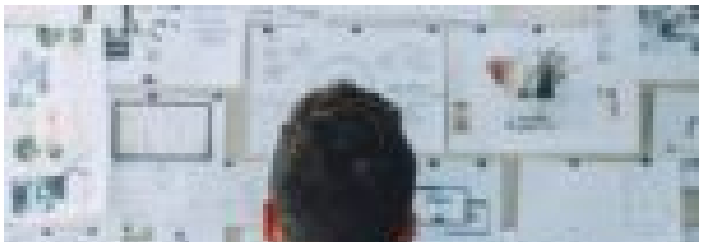


Business and DevOps value streams need better alignment (https://sdtimes.com/devops/business-and-devops-value-streams-need-better-alignment/)

SD Times news digest: Cloud Security Alliance's pillars of DevSecOps automation, dotData Stream, and Dynatrace announces AI observability for Kubernetes (https://sdtimes.com/softwaredev/sd-times-news-digest-cloud-security-alliances-pillars-of-devsecops-automation-dotdata-stream-and-dynatrace-announces-ai-observability-for-kubernetes/)



ShiftLeft focuses on developer productivity with next generation static analysis solution (https://sdtimes.com/security/shiftleft-focuses-on-developer-productivity-with-next-generation-static-analysis-solution/)



DevOps Report: Testing is Everything (https://sdtimes.com/devops/devops-report-testing-is-everything/)

SD Times

- About Us (https://d2emerge.com/)
- Contact Us (https://d2emerge.com/about/)
- Privacy Policy (https://sdtimes.com/privacy-policy/)
- Site Map (https://sdtimes.com/site-map/)
- Advertise (https://d2emerge.convertflowpages.com/advertisesdtimes)
- Subscribe (https://sdtimes.com/subscribe-to-sd-times-magazine/)
- Manage My Preferences (https://sdtimes.com/subscriptionupdate/)

Subscribe to SD Times

(https://sdtimes.com/sd-times-july-2020/)

Ready for your SD Times magazine? It's just a click away!

Subscribe (https://sdtimes.com/subscribe-to-sd-times-magazine/)

- Read Current Issue (https://sdtimes.com/sd-times-july-2020/)
- Read Back Issues (https://sdtimes.com/back-issues/)

Tweets by @sdtimes (https://twitter.com/sdtimes)

Subscribe (https://sdtimes.com/subscribe-to-sd-times-magazine/) Contact Us (https://d2emerge.com/about/)
Site Map (https://sdtimes.com/site-map/) Privacy Policy (https://sdtimes.com/privacy-policy/)